(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 753 824**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04W 36/00 (2009.01)
H04W 36/08 (2009.01)
H04W 88/02 (2009.01)
H04W 88/08 (2009.01)
H04W 92/20 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.09.2016 PCT/SE2016/050879**

(87) Fecha y número de publicación internacional: **13.04.2017 WO17061924**

(96) Fecha de presentación y número de la solicitud europea: **20.09.2016 E 16775001 (7)**

(97) Fecha y número de publicación de la concesión europea: **07.08.2019 EP 3360359**

(54) Título: **Nodos para uso en una red de comunicación y métodos para operar los mismos**

(30) Prioridad:

08.10.2015 US 201562238966 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.04.2020

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

AXÉN, RASMUS y
NORRMAN, KARL

(74) Agente/Representante:

LINAGE GONZÁLEZ, Rafael

DESCRIPCIÓN

Nodos para uso en una red de comunicación y métodos para operar los mismos

Campo técnico

Este documento se refiere a una red de comunicación, y en particular a técnicas que se refieren al traspaso de un dispositivo terminal entre los nodos de acceso de radio en la red de comunicación.

Antecedentes

En redes de comunicación de evolución a largo plazo (LTE), las comunicaciones entre el equipamiento de usuario (UE) y un eNB encriptado y parcialmente protegido de integridad. Las claves de integridad y encriptación derivan de una clave raíz común llamada K_{eNB} que se comparte entre el UE y el eNB. El K_{eNB} es único al par Pcell-UE, donde Pcell es la célula primaria que el UE utiliza como una célula “maestra“ cuando se comunica con un eNB. Desde que el UE solo utiliza una Pcell para comunicar con un eNB, el K_{eNB} es también único para el par eNB-UE. Esto es, el mismo K_{eNB} nunca se utiliza para proteger el tráfico entre el UE y dos eNB diferentes. El razonamiento detrás de este diseño es prevenir que un atacante que ha ganado acceso a o conocimiento de un K_{eNB} que se utiliza entre un UE a un primer eNB obtenga utilidad de ese K_{eNB} cuando intenta romper la encriptación o integridad en el tráfico entre el UE y un eNB diferente.

Para asegurar que el K_{eNB} es único por cada par eNB-UE, K_{eNB} se cambia durante el traspaso entre dos eNB. para la simplicidad, K_{eNB} realmente se cambia en todos los traspasos inter-LTE (por ejemplo, traspaso entre células), aun cuando los eNB de origen y eNB de destino es el mismo nodo.

La singularidad del par UE-KeNB durante el traspaso se consigue por el hecho de que el UE y el eNB de origen derivan un nuevo K_{eNB} (denotado K_{eNB}*) a partir del K_{eNB} actual, el identificador de célula física (PCI) de la célula primera de destino (PCell) y la frecuencia de enlace descendente de célula física de destino (por ejemplo, el número de canal de frecuencia de radio absoluto evolucionado para el enlace descendente, EARFCN-DL). Esto se especifica en la cláusula 7.2.8. sw 3GPP TS 33 401 “3GPP evolución de arquitectura de sistema (SAE); arquitectura de seguridad”, versión 12.14.0 (2015-03).

Mas específicamente, la entrada a la función de derivación de clave (KDF) para derivar K_{eNB}* es:

FC = 0x13

P0 = PCI (PCI de destino)

L0 = largo de PCI (es decir, 0x00 0x02)

P1 = EARFCN-DL (frecuencia de enlace descendente de célula física de destino)

L1 largo de EARFCN-DL (es decir, 0x00 0x02)

Un traspaso entre dos eNB sin la intervención de red central, un llamado traspaso X2, se describe posteriormente con referencia a la figura 1. Los traspasos pueden realizarse después de que el UE haya completado todos los procedimientos necesarios para activar la seguridad del control de recurso de radio (RRC) y del estrato de no-acceso (NAS). El traspaso X2 se inicia por el eNB de origen 2 calculando una clave K_{eNB}* desde la K_{eNB} activa actual, compartida entre el eNB de origen 2 y el UE 3, y enviándola junto con las capacidades de seguridad de UE al eNB de destino 4 en un mensaje de solicitud de traspaso 5. El eNB de destino 4 responde con la información de configuración requerida 5 para la conexión UE. Esta información incluye los algoritmos elegidos que deberían utilizar el eNB de destino 4 y el UE 3. El eNB de origen 2 entonces avanza la respuesta al UE 3 (señal 6), y el UE 3 confirma el traspaso con un mensaje de fin 7 al eNB de destino 4. En el último paso, el eNB de destino 4 recupera una nueva clave llamada la clave de siguiente salto (NH) desde una entidad de administración de movilidad (MME). El NH se deriva desde una clave K_{ASME} (una clave base que se comparte por el UE y MME) y el NH se utiliza como una base para el cálculo de K_{eNB}* en el siguiente evento de traspaso.

En algunos escenarios el eNB de origen no tiene una clave NH “fresca” cuando realiza un traspaso, y en vez de eso el eNB puede crear un nuevo K_{eNB}* a partir del K_{eNB} actual. Esto se llama una derivación de clave vertical. Una clave NH se denomina que es “fresca” cuando no se ha utilizado previamente.

La clave K_{eNB}* en sí no se envía desde el eNB al UE, y en vez un elemento de información (IE) indicando si el K_{eNB}*se deriva verticalmente (es decir, existe un NH fresco) u horizontalmente (no existe NH fresco en el eNB) se envía al UE. Este elemento de información se llama NCC (contador de concatenación de siguiente salto) y se incluye en el mensaje de reconfiguración RRC. El NCC es un valor entre 0-7. Si se pisa el NCC, entonces el UE sabe que debe realizarse una derivación de llave vertical, y cuando el NCC es el mismo que el NCC asociado con el K_{eNB}

actualmente activo, el UE en vez de eso realizara una derivación de clave horizontal.

Una moda en las redes de hoy en día es que la operadora añada más frecuencias y reduzca al tamaño de las células para aumentar la capacidad de banda ancha móvil. Esto lleva a un aumento en las reconfiguraciones de UE y acciones de movilidad.

La habilidad de mover rápido o resumir una sesión de UE entre células se vuelve cada vez más importante con el fin de caber los patrones de tráfico asociados con explosiones de datos cortos. Sin embargo, desde que las claves de encriptación e integridad derivan desde una clave base (K_{eNB}) que está atada a la célula primaria (mediante el uso del EARFCN-DL de la célula primaria y el PCI en la derivación de la clave K_{eNB}), cada vez que el UE se mueve desde esa Pcell o se reconecta en otra Pcell se debe realizar una renegociación de clavee antes de que se siga con el tráfico. Esto causa un problema puesto que la renegociación de K_{eNB} consume considerable memoria y ciclos de procesador, y en particular resulta en que las claves de encriptación e integridad tienen que derivarse desde el nuevo K_{eNB}. Cuando se actualiza la nueva clave de encriptación, algunos paquetes ya encriptados deben ser cargados, desencriptados utilizando la vieja clave de encriptación y entonces re-encriptados utilizando la nueva clave de encriptación. Un problema análogo es que los paquetes ya protegidos de integridad igualmente necesitan re-protegerse utilizando la nueva clave de protección de integridad. Esto añade retraso que reduce la experiencia del usuario final. Además, complica la implementación del eNB, llevando a un riesgo mayor de errores de implementación y un coste mayor para el mantenimiento de código.

La solicitud de patente número WO 00/41427 A1 divulga la reutilización de asociaciones de seguridad para mejorar la realización de traspaso. Cuando una unidad móvil se somete a un traspaso desde una primera estación base a una segunda estación base, se verifica si la primera y la segunda estación base pertenecen al mismo dominio administrativo. Si pertenecen al mismo dominio, la primera estación base manda información de asociación de seguridad a la segunda. Si no, la unidad móvil necesita negociar una nueva asociación de seguridad con la segunda estación base.

El problema anterior se describe en el contexto de la manera que se maneja la seguridad en LTE, aunque el problema puede también ser evidente en otros tipos de redes de comunicación. Se apreciará que la necesidad de optimizar el procesamiento de seguridad es común a muchos tipos diferentes de redes.

Por ello, hay una necesidad de mejoras en la manera en que se maneja la seguridad cuando ocurre un traspaso entre dos eNB.

Sumario

Según un primer aspecto, se proporciona un método para operar un primer nodo de acceso de radio en una red de comunicación, como se define en la reivindicación 1.

Según un segundo aspecto, se proporciona un primer nodo de acceso de radio para utilizar en una red de comunicación, como se define en la reivindicación 13.

Según un cuarto aspecto, se proporciona un método para operar un dispositivo de comunicación, según la reivindicación 10.

Según un quinto aspecto, se proporciona un dispositivo de comunicación, según la reivindicación 22.

Realizaciones particulares pueden incorporar uno o más aspectos proporcionados anteriormente y pueden combinarse elementos de ciertos aspectos.

Breve descripción de los dibujos

Algunas realizaciones de las técnicas introducidas en este documento se describen posteriormente con referencia a las siguientes figuras, en las que:

la figura 1 ilustra la señalización en un traspaso entre un eNB de origen y un eNB de destino en una red LTE;

la figura 2 es un ejemplo no limitante de un diagrama de bloques de una red de comunicaciones celulares LTE;

la figura 3 es un diagrama de bloques de un dispositivo de comunicación según una realización;

la figura 4 es un diagrama de bloques de un nodo de acceso de radio según una realización;

la figura 5 es un diagrama de bloques de un nodo de red central según una realización;

la figura 6 es un diagrama de flujo que ilustra un método para operar un nodo de acceso de radio según una

realización;

la figura 7 es un diagrama de flujo que ilustra un método para operar un dispositivo de comunicación según una realización;

la figura 8 es un diagrama de flujo que ilustra un método para operar un nodo de acceso de radio según otra realización;

la figura 9 es un diagrama de flujo que ilustra un método para operar un nodo de una red de comunicación según una realización;

la figura 10 ilustra un procedimiento de traspaso ejemplar en el que se utilizan las técnicas descritas aquí;

la figura 11 es un diagrama de bloques de un primer nodo de acceso de radio según una realización;

la figura 12 es un diagrama de bloques de un dispositivo de comunicación según otra realización;

la figura 13 es un diagrama de bloques de un segundo nodo de acceso de radio según una realización;

la figura 14 es un diagrama de bloques de un nodo según una realización adicional;

la figura 15 es un diagrama de bloques de un primer nodo de acceso de radio según todavía otra realización;

la figura 16 es un diagrama de bloques de un dispositivo de comunicación según todavía otra realización;

la figura 17 es un diagrama de bloques de un segundo nodo de acceso de radio según todavía otra realización; y

la figura 18 es un diagrama de bloques de un nodo según todavía otra realización.

Descripción detallada

Lo siguiente establece detalles específicos, tales como realizaciones particulares con fines de explicación y no de limitación. Pero se apreciará por uno experto en la técnica que pueden emplearse otras realizaciones aparte de estos detalles específicos. En algunos casos, se omiten descripciones detalladas de métodos, nodos, interfaces, circuitos y dispositivos bien conocidos para no ocultar la descripción con detalles innecesarios. Los expertos en la técnica apreciaran que las funciones descritas aquí pueden implementase en uno o más nodos utilizando circuitería de equipo físico informático (por ejemplo, puertas lógicas analógicas y/o discretas interconectadas para realizar una función especializada, ASIC, PLA, etc.) y/o utilizando programas de equipo lógico informático y datos en conjunto con uno o más microprocesadores digitales u ordenadores de objetivo general. Nodos que comunican utilizando la interfaz de aire también tienen circuitería de comunicaciones de radio adecuada. Además, en caso apropiado, la tecnología se puede considerar adicionalmente para ser materializada totalmente dentro de cualquier forma de memoria leíble por ordenador, tal como memoria de estado sólido, disco magnético o disco óptico que contiene un conjunto apropiado de instrucciones de ordenador que podrían hacer que un procesador lleve a cabo las técnicas descritas aquí.

La implementación de equipo físico informático puede incluir o abarcar, sin limitación, equipo físico informático de procesador de señal digital (DSP), un procesador de conjunto de instrucciones reducido, circuitería de equipo físico informático (por ejemplo, digital o analógico) que incluye pero no limitado a circuitos integrados específicos de aplicación (ASIC) y/o matrices de puertas programables de campo (FPGA) y (en caso apropiado) máquinas de estado capaces de realizar tales funciones.

En términos de implementación de ordenador, un ordenador se entiende generalmente para comprender uno o más procesadores, una o más unidades de procesamiento, uno o más módulos de procesamiento o uno o más controladores, y los términos de ordenador, procesador, unidad de procesamiento, módulo de procesamiento y controlador pueden emplearse de manera intercambiable. Cuando se proporciona por un ordenador, procesador, unidad de procesamiento, módulo de procesamiento o controlador, las funciones pueden proporcionarse por un único y delicado ordenador, procesador, unidad de procesamiento, módulo de procesamiento o controlador, por un único y compartido ordenador, procesador, unidad de procesamiento, módulo de procesamiento o controlador, o por una pluralidad de ordenadores, procesadores, unidades de procesamiento, módulos de procesamiento o controladores individuales, algunos de los cuales pueden compartirse o distribuirse. Además, estos términos también se refieren a otro equipo físico informático capaz de realizar tales funciones y/o equipo lógico informático de ejecución, tal como el equipo físico informático de ejemplo citado anteriormente.

Aunque en la descripción posterior se utiliza el término equipamiento de usuario (UE), debería entenderse por los expertos en la técnica que “UE” es un término no limitante que comprende cualquier dispositivo móvil, dispositivo de comunicación, dispositivo de comunicación inalámbrica, dispositivo terminal o nodo equipado con una interfaz de

radio que permite al menos una de: transmitir señales en enlace ascendente (UL) y recibir y/o medir señales en enlace descendente (DL). Un UE aquí puede comprender un UE (en su sentido general) capaz de operar o al menos realizar medidas en una o más frecuencias, frecuencias portadoras, portadoras de componentes o bandas de frecuencia. Puede ser un "UE" operando en tecnología de acceso de única radio o multi radio (RAT) o modo multi estándar. Así como "UE", los términos generales "dispositivo terminal", "dispositivo de comunicación" y "dispositivo de comunicación inalámbrica", se utilizan en la siguiente descripción, y se apreciará que dicho dispositivo puede o no ser "movible" en el sentido de que se lleva por un usuario. En vez de eso, el término "dispositivo terminal" (y los términos generales alternativos establecidos anteriormente) abarca cualquier dispositivo que es capaz de comunicarse con redes de comunicación que operan según uno o más estándares de comunicación móvil, tales como sistema global para comunicaciones móviles, GSM, sistema de telecomunicaciones móvil universal (UMTS), evolución a largo plazo, LTE, etc. También se apreciará que un UE puede comprenden un módulo de identidad de suscripción universal (USIM) en una tarjeta inteligente o implementado directamente en el UE, por ejemplo como un equipo lógico informático o un circuito integrado. Las operaciones descritas aquí pueden implementarse parcial o completamente en el USIM o fuera del USIM.

Una o más células están asociadas con una estación base, donde una estación base comprende en un sentido general cualquier nodo de red que transmite señales de radio en el enlace descendente y/o recibe señales de radio en el enlace ascendente. Algunas estaciones base de ejemplo, o términos utilizados para describir estaciones base, don eNodoB, eNB, NodoB, macro/micro/pico/femto estación base de radio, eNodoB de casa (también conocido como estación base femto), relé, repetidor, sensor, transmitir solo nodos de radio o recibir solo nodos de radio. Una estación base puede operar o al menos realizar medidas en una o más frecuencias, frecuencias portadoras o bandas de frecuencia y puede ser capaz de agregar portadoras. También puede ser una única tecnología de acceso de radio (RAT), multi-RAT, o nodo multi estándar, por ejemplo utilizando los mismos o diferentes módulos de banda base para diferentes RAT.

A no ser que se indique aquí, la señalización descrita es o bien mediante enlaces directos o enlaces lógicos (por ejemplo, mediante protocolos de capa alta y/o mediante uno o más nodos de red).

La figura 2 muestra un diagrama de ejemplo de una arquitectura de red de acceso de radio terrestre de sistema de telecomunicaciones móviles universal (UMTS) evolucionado (E-UTRAN) como parte de un sistema de comunicaciones basadas en LTE 32 al que se aplican las técnicas descritas aquí. Nodos en una red central 34 parte del sistema 32 incluyen una o más entidades de administración de movilidad (MME) 36, un nodo de control de clave para la red de acceso LTE, y una o más pasarelas de servicio (SGW) 38 que enruta y remite paquetes de datos de usuario mientras actúan como ancla de movilidad. Comunican con estaciones base o nodos de acceso de radio 40 referidos como eNB en el LTE, sobre una interfaz, por ejemplo una interfaz S1. Los eNB 40 pueden incluir las mismas o diferentes categorías de eNB, por ejemplo macro eNB, y/o micro/pico/femto eNB. Los eNB 40 comunican entre ellos sobre una interfaz inter-nodo, por ejemplo una interfaz X2. La interfaz S1 y la interfaz S2 se definen en el estándar LTE. Se muestra un UE 42, y un UE 42 puede recibir de enlace descendente desde y enviar datos de enlace ascendente a una de las estaciones base 40, denominándose esa estación base 40 la estación base de servicio del UE 42.

La figura 3 muestra un dispositivo de comunicación/dispositivo terminal (UE) 42 que puede adaptarse o configurarse para operar según uno o más de los ejemplos no limitantes de las realizaciones descritas. El UE 42 comprende un procesador o unidad de procesamiento 50 que controla la operación del UE 42. La unidad de procesamiento 50 está conectada a una unidad transceptora 52 (que comprende un receptor y un transmisor) con antenas asociadas 54 que se utilizan para transmitir señales y recibir señales hace un nodo de acceso de radio 40 en la red 32. El UE 42 también comprende una memoria o unidad de memoria 56 que está conectada a la unidad de procesamiento 50 y que contiene instrucciones o códigos ejecutables de ordenador por la unidad de procesamiento 50 y otra información o datos requeridos para la operación del UE 42.

La figura 4 muestra un nodo de acceso de radio (por ejemplo, una estación base de red celular tal como un NodoB o un eNodoB, eNB) 40 que puede adaptarse o configurarse para operar según las realizaciones de ejemplo descritas. El nodo de acceso de radio 40 comprende un procesador o unidad de procesamiento 60 que controla la operación del nodo de acceso de radio 40. La unidad de procesamiento 60 está conectada a una unidad transceptora 62 (que comprende un receptor y un transmisor) con antenas asociadas 64 que se utilizan para transmitir señales a, y recibir señales de, los UE 42 en la red 32. El nodo de acceso de radio 40 también comprende una memoria o unidad de memoria 66 que está conectado a la unidad de procesamiento 60 y que contiene instrucciones o códigos de ordenador ejecutables por la unidad de procesamiento 60 y otra información o datos requeridos para la operación del nodo de acceso de radio 40. El nodo de acceso de radio 40 también incluye componentes y/o circuitos 68 para permitir el nodo de acceso de radio 40 para cambiar información con otro nodo de acceso de radio 40 (por ejemplo, mediante una interfaz X2), y/o con un nodo de red central 36, 38 (por ejemplo, mediante una interfaz S1). Se apreciará que las estaciones base para utilizar en otros tipos de red (por ejemplo, UTRAN o RAN WCDMA) incluirán componentes similares a aquellos mostrados en la figura 4 y circuito de interfaz apropiado 68 para permitir comunicaciones con los nodos de acceso de radio en aquellos tipos de redes (por ejemplo, otras estaciones base, nodos de administración de movilidad y/o nodos en la red central). Se apreciará que un nodo de acceso de radio 40 puede implementarse como un número de funciones distribuidas en la red de acceso de radio (RAN).

La figura 5 muestra un nodo de red central 36, 38 que puede utilizarse en las realizaciones descritas de ejemplo. El nodo 36, 38 podría ser un MME 36, una SGW 38, u otro tipo de nodo de red central (por ejemplo, un controlador de red de radio, RNC). El nodo 36, 38 comprende una unidad de procesamiento 70 que controla la operación del nodo 36, 38. La unidad de procesamiento 70 está conectada a circuitería y/o componentes de interfaz 72 por permitir al nodo 36, 38 intercambiar información con nodos de red en la red de acceso de radio (RAN), por ejemplo, nodos de acceso de radio 40, que se asocia (que es típicamente mediante la interfaz S1) y/o con otros nodos en la parte de red central de la red. El nodo 36, 38 también comprende una unidad de memoria 74 que está conectada a la unidad de procesamiento 70 y que guarda programa y otra información y datos requeridos para la operación del nodo 36, 38.

También se apreciará que solo los componentes del UE 42, nodo de acceso de radio 40 y nodo de red 36, 38 descritos y presentados en el contexto de las realizaciones divulgadas aquí se ilustran en las figuras 3, 4 y 5.

Aunque las realizaciones de la presente divulgación serán principalmente descritas en el contexto de LTE, se apreciará por aquellos expertos en la técnica que los problemas y soluciones descritos aquí se aplican igualmente a otros tipos de redes de acceso inalámbricas y equipamientos de usuario (UE) implementando otras tecnologías de acceso y estándares, y por ello LTE (y la otra terminología específica de LTE utilizada aquí) deberían solo verse como ejemplos de las tecnologías a las que se aplican las técnicas.

Como se menciona anteriormente, hay problemas con el manejo actual de la seguridad en una red de comunicación LTE, particularmente refiriéndose al manejo de la seguridad durante el procedimiento de traspaso entre eNB. Las técnicas proporcionadas posteriormente por ello proporcionan mejoras en la manera en que la seguridad se maneja cuando ocurre un traspaso entre eNB seleccionados.

En particular las técnicas descritas aquí proporcionan que la misma clave base (por ejemplo, K_{eNB}) pueda utilizarse después de un cambio (traspaso) desde una Pcell a otra si se considera segura la continua utilización del K_{eNB}. Si el K_{eNB} puede utilizarse después de un cambio, se proporciona señalización desde el eNB de origen o el eNB de destino para indicar al UE que el UE debería seguir utilizando K_{eNB} después del traspaso.

En realizaciones particulares puede considerarse seguro seguir utilizando el K_{eNB} después de un traspaso si el eNB de origen y el eNB de destino son parte de la misma “zona se seguridad“. Una “zona de seguridad“ puede definirse como un conjunto de eNB que están configurados o dispuestos de tal manera que, si un atacante fuera a hackear, acceder o asaltar de otro modo uno de los eNB en el conjunto, el atacante también debería ser capaz de hackear, acceder o asaltar de otro modo uno de los otros sin un esfuerzo adicional sustancial. Por ejemplo, una red de acceso de radio (RAN) pueden “nubificarse“, donde múltiples eNB pueden funcionar como máquinas virtuales separadas en el mismo equipo físico informático. En este caso, un atacante que gana acceso al equipo físico informático puede ganar acceso a cualquiera o todos los eNB que funcionan en ese equipo físico informático. En una RAN alternativa “nubificada“, múltiples eNB pueden implementarse en respectivos contendores dentro de la misma máquina virtual. De nuevo, un atacante que gana acceso a la máquina virtual puede acceder a cualquiera de todos los eNB que se están haciendo funcionar por esa máquina virtual. Un ejemplo más de eNB estando considerados para están dentro de una zona de seguridad es cuando los eNB se implementan en respectivos circuitos/placas de componentes en el mismo estante de ordenador físico. Generalmente, una zona de seguridad puede considerarse como un conjunto de eNB que están en la misma localización física y/o virtual. Alternativamente, los eNB que son partes de una “zona de seguridad“ particular pueden configurarse o seleccionarse por la operadora de la red, por ejemplo en base a la valoración del riesgo de la seguridad de red que está comprometida si un eNB en la zona se hackea o accede.

Un método ejemplar de operar un nodo de acceso de radio (por ejemplo, un eNB en una red LTE) 40 según las técnicas descritas aquí se muestra en la figura 6. El nodo de acceso de radio 40 también se refiere posteriormente como el “primer“ nodo de acceso de radio. En este método, el primer nodo de acceso de radio 40 es la célula de origen para un dispositivo de comunicación (por ejemplo, un UE) 42.

En un primer paso, el paso 601, el primer nodo de acceso de radio 50 determina si una primera clave de base, referida como primera clave base AS (por ejemplo, K_{eNB}) posteriormente que se utiliza para determinar una primera clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y el primer nodo de acceso de radio 40 puede utilizarse por un segundo nodo de acceso de radio 40 para determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y el segundo nodo de acceso de radio.

En algunas realizaciones el paso 601 comprende determinar que la primera clave base puede ser utilizada por el segundo nodo de acceso de radio si el primero nodo de acceso de radio y el segundo nodo de acceso de radio son parte de la misma zona de seguridad. En algunas realizaciones, el primer nodo de acceso de radio y el segundo nodo de acceso de radio son parte de la misma zona de seguridad si el primer nodo de acceso de radio y el segundo nodo de acceso de radios radio: (a) están funcionando como máquinas virtuales separadas en el mismo equipo físico informático; (b) son dos contenedores dentro de la misma máquina virtual; (c) están implementados en placas en el mismo estante físico; (d) se determina por política de seguridad que pertenecen a la misma zona de seguridad;

o (e) están localizados físicamente en el mismo lugar.

El paso 601 puede realizarse examinando una lista o configuración local en el primer nodo de acceso de radio, o por pedir información de otro nodo (por ejemplo, como se describe posteriormente con referencia a la figura 9. En este respecto, el paso 601 puede además comprender enviar una petición de información en el segundo nodo de acceso de radio a otro nodo en la red de comunicación (por ejemplo, otro nodo de acceso de radio, eNB, o un nodo en la red central, por ejemplo, un MME 36), y recibir una respuesta a esa petición que contiene información en el segundo nodo de acceso de radio. La información puede indicar si la primera clave de base puede ser utilizada por el segundo de nodo de acceso de radio, o la información puede permitir el primer nodo de acceso de radio 40 para determinar si la primera clave base puede ser utilizada por el segundo nodo de acceso de radio.

Si en el paso 601 se determina que la primera clave base puede utilizarse por el segundo nodo de acceso de radio, el método además comprende el paso de enviar la primera clave base al segundo nodo de acceso de radio durante el traspaso del dispositivo de comunicación desde el primer nodo de acceso de radio al segundo nodo de acceso de radio (paso 603).

En adición, aunque no se muestra en la figura 6, si la primera clave base puede utilizarse por el segundo nodo de acceso de radio, el primer nodo de acceso de radio también manda una indicación al dispositivo de comunicación que la primera clave base se debe utilizar para determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y el segundo nodo de acceso de radio. Esta indicación puede incluirse en un mensaje que se refiere al traspaso del dispositivo de comunicación desde el primer nodo de acceso de radio al segundo nodo de acceso de radio. El mensaje puede ser un mensaje de reconfiguración de control de recurso de radio, RRC.

Si en el paso 601 se determina que la primera clave base no se puede utilizar por el segundo nodo de acceso de radio, el primer nodo de acceso de radio 40 determina una segunda clave base desde la primera clave base (paso 605). Esta derivación de clave puede llevarse a cabo de una manera convencional (por ejemplo, utilizando derivación horizontal o vertical). El primer nodo de acceso de radio 40 entonces manda la segunda clave base al segundo nodo de acceso de radio durante el traspaso del dispositivo de comunicación desde el primer nodo de acceso de radio al segundo nodo de acceso de radio (paso 607). En este caso el primer nodo de acceso de radio 40 puede también manda una indicación al dispositivo de comunicación para hacer que el dispositivo de comunicación determine una segunda clave base desde la primera clave base para utilizar con el segundo nodo de acceso de radio.

En algunas realizaciones, el primer nodo de acceso de radio 40 puede también enviar una indicación de un algoritmo de generación de clave de encriptación que se utilizó para determinar la primera clave de encriptación desde la primera clave base al segundo nodo de acceso de radio 40.

Como se nota posteriormente, en algunas realizaciones el primer nodo de acceso de radio y el segundo nodo de acceso de radio pueden compartir un estado o función PDCP.

La figura 7 ilustra un método de operar un dispositivo de comunicación (por ejemplo, un UE) 42 según las técnicas presentadas aquí. El dispositivo de comunicación 42 se sirve por un primer nodo de acceso de radio 40 (por ejemplo, un eNB).

En un primer paso, el paso 701, en el traspaso del dispositivo de comunicación desde un primer nodo de acceso de radio (por ejemplo, eNB) 40 a un segundo nodo de acceso de radio (por ejemplo, eNB) 40, el dispositivo de comunicación recibe una indicación de si una primera clave base que se utiliza para determinar una primera clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y el primer nodo de acceso de radio se pueden utilizar para determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y el segundo nodo de acceso de radio.

Esta indicación se puede recibir desde el primer nodo de acceso de radio 40 o el segundo nodo de acceso de radio 40.

Si la indicación recibida indica que la primera clave base se puede utilizar para determinar una segunda clave de encriptación (en el paso 703), el dispositivo de comunicación 42 determina una segunda clave de encriptación desde la primera clave base (paso 705). Esta segunda clave de encriptación puede entonces utilizarse para encriptar comunicaciones entre el dispositivo de comunicación y el segundo nodo de acceso de radio.

Si la indicación recibida indica que la primera clave base no se puede utilizar para determinar una segunda clave de encriptación (en el paso 703), el dispositivo de comunicación determina una segunda clave base desde la primera clave base (paso 707). Esta segunda clave base puede derivarse de una manera convencional, por ejemplo, utilizando derivación de clave horizontal o vertical.

El dispositivo de comunicación 42 entonces determina una segunda clave de encriptación para encriptar

comunicaciones entre el dispositivo de comunicación y el segundo nodo de acceso de radio desde la segunda clave base (paso 709).

En algunas realizaciones, la indicación recibida en el paso 701 está en un mensaje que se refiere al traspaso del dispositivo de comunicación desde el primer nodo de acceso de radio al segundo nodo de acceso de radio el mensaje puede ser un mensaje de reconfiguración de control de recurso de radio, RRC.

Un método de operar un nodo de acceso de radio (por ejemplo, un eNB en una red LTE) 40 según las técnicas recibidas aquí se muestra en a figura 8. El nodo de acceso de radio 40 también se denomina “segundo“ nodo de acceso de radio posteriormente, y corresponde a la célula de destino para el dispositivo de comunicación.

En un primer paso, el paso 901, el segundo nodo de acceso de radio 40 recibe una primera clave base desde un primer nodo de acceso de radio 40 durante el traspaso de un dispositivo de comunicación desde el primer nodo de acceso de radio al segundo nodo de acceso de radio. El segundo nodo de acceso de radio 40 también recibe desde el primer nodo de acceso de radio una indicación de un algoritmo de generación de clave de encriptación que se utilizó para determinar una primera clave de encriptación desde una primera clave base (paso 903). El segundo nodo de acceso de radio 40 entonces utiliza la primera clave base y el algoritmo de generación de clave de encriptación indicado para determinar una clave de encriptación.

La primera clave base y algoritmo de generación de clave de encriptación indicado deberán haber sido utilizados previamente por el primer nodo de acceso de radio para generar una clave de encriptación para utilizar en comunicaciones de encriptación entre el primer nodo de acceso de radio y el dispositivo de comunicación, y entonces determinar una clave de encriptación utilizando la primera clave base y el algoritmo de generación de clave de encriptación indicado, el segundo nodo de acceso de radio 40 generará la misma clave de encriptación como la que se utilizó por el primer nodo de acceso de radio 40.

Un método ejemplar de operar un nodo de red según otra realización de las técnicas descritas aquí se muestra en la figura 9. El nodo podría ser un nodo en la parte de red central de la red de comunicación (y por ejemplo el nodo podría ser un MME 36), o un nodo en el RAN de la red de comunicación (por ejemplo, un eNB 40, o una función o componente que es parte de una arquitectura eNB distribuida). Este nodo puede ser responsable para tomar una decisión en compartir una clave base y enviar la decisión al nodo de acceso de radio requerido.

Además, en un primer paso, paso 901, el nodo recibe una petición desde un primer nodo de acceso de radio en la red de comunicación para información en un segundo nodo de acceso de radio en la red de comunicación. La información requerida se refiere a si la primera clave base que se utilizó para determinar una primera clave de encriptación para encriptar comunicaciones entre un dispositivo de comunicación y el primer nodo de acceso de radio pueden utilizarse para determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y el segundo nodo de acceso de radio.

El nodo recupera u obtiene la información requerida y manda la información al primer nodo de acceso de radio 40 (paso 903), la información indicando si la primera clave base puede utilizarse por el segundo nodo de acceso de radio.

En algunas realizaciones, después de recibir la petición por información, el nodo puede determinar si la primera clave base puede utilizarse por un segundo nodo de acceso de radio. Esta determinación puede comprender el nodo determinando que la primera clave base puede utilizarse por el segundo nodo de acceso de radio si el primer nodo de acceso de radio y el segundo nodo de acceso de radio son parte de la misma zona de seguridad. El primer nodo de acceso de radio y el segundo nodo de acceso de radio pueden considerarse como parte de la misma zona de seguridad si el primer nodo de acceso de radio y el segundo nodo de acceso de radio: (a) están funcionando como máquinas virtuales separadas en el mismo equipo físico informático; (b) son dos contenedores dentro de la misma máquina virtual; (c) están implementados en placas en el mismo estante físico; (d) se determina por política de seguridad que pertenecen a la misma zona de seguridad; o (e) están localizados físicamente en el mismo lugar.

Una realización específica de las técnicas presentadas aquí en el contexto de un traspaso X2 en una red LTE se muestra en la figura 10. Debería notarse que los principios descritos posteriormente pueden aplicarse a traspasos S1 u otros tipos de traspasos que utilizan seguridad y/o estructuras de mensaje similares.

La figura 10 muestra la señalización involucrada en un traspaso X2 de un dispositivo terminal (UE 42) desde un primer nodo de acceso de radio 40 que controla una célula maestra de origen (denotada “célula de origen” 78 en la figura 10), por ejemplo, un primer eNB 40, a un segundo nodo de acceso de radio 40 que controla una célula maestra de destino (denotada “célula de destino” 79 en la figura 10), por ejemplo, un segundo eNB 40. El término célula maestra aquí se refiere a una célula que el UE 42 necesita haber establecido con un eNB 40 para considerarse conectada a ese eNB 40, y podría, por ejemplo, ser una Pcell (célula primaria).

La estructura del traspaso X2 generalmente comprende los siguientes pasos: un nodo en el RAN (por ejemplo, la célula de origen 40 en el ejemplo de la figura 10) decide que debe tener lugar un traspaso del UE 42 (paso 80 en la

figura 10), el eNB que soporta o aloja la célula de origen 78 pide al eNB 78 que soporta o aloja la célula de destino 79 que se prepare para el traspaso (paso 84), el eNB 40 que aloja la célula de destino 79 reconoce positivamente la petición (paso 86), el eNB 40 que aloja la célula de origen 78 pide al UE 42 que reconfigure la conexión RRC para la célula de destino 79 (paso 88), y finalmente el UE 42 completa el traspaso informando al eNB 40 que aloja la célula de destino 79 (paso 90).

De este modo, en el paso 80 un nodo en la RAN decide que el UE 42 necesita cambiar desde la célula de origen 78 a la célula de destino 79. En este ejemplo el nodo que toma esta decisión es el eNB 40 que aloja la célula de origen 78, aunque es posible que la decisión se tome en un nodo diferente. La decisión se toma típicamente debido a razones de cobertura, por ejemplo calidad baja de señal, pero podría tomarse debido a otras razones tales como carga en la célula. El paso 80 se generalmente convencional y no se describirá más.

Antes de pedir al eNB 40 que aloja la célula de destino 79 que se prepare para un traspaso (que está representado por el envío del mensaje petición de preparación de traspaso 84 desde el eNB 40 que aloja la célula de origen 78 al eNB 40 que aloja la célula de destino 79), el eNB 40 que aloja la célula de origen 78 determina si la clave base AS actual (utilizada por el UE 42 y el eNB 40 para derivar claves de protección de encriptación y seguridad para proteger el tráfico transmitido en la célula de origen 78) puede utilizarse por el UE 42 y el eNB 40 que aloja la célula de origen 78 sin comprender seguridad. Esto se muestra como el paso 82 en la figura 10 (DeterminarMantenerClave). La clave base AS, por ejemplo K_{eNB}, se utiliza para determinar una clave de encriptación para encriptar comunicaciones entre el UE 42 y el eNB 40 que aloja la célula de origen 78.

La decisión en el paso 82 puede basarse en uno o más factores, y en particular si el eNB 40 que aloja la célula de destino 79 está en la misma “zona de seguridad“ que el eNB que aloja la célula de origen 78. Se describe una zona de seguridad anteriormente. La operadora del RAN puede ser capaz de configurar zonas de seguridad (por ejemplo, que células o eNB están en cada zona de seguridad). Puede haber una lista de células/eNB que están en cada zona de seguridad (que cada eNB 40 puede estar configurado con lo que puede accederse o consultarse por eNB), y la decisión en el paso 82 puede comprender determinar si la célula de destino 79 está en la misma lista que la célula de origen 78. Las células/eNB en cada zona de seguridad puede identificarse de numerosas maneras, por ejemplo, utilizando PCI específicos, identificadores para eNB 40 en el RAN, direcciones de protocolo de internet (IP), nombres de dominio cualificados completamente (FQDN) y/o direcciones de control de acceso de media (MAC) que están asociados con cada célula/eNB, y/o por rangos de nombres o direcciones (por ejemplo, cualquier célula/eNB que tiene una dirección en el rango específico se considera parte de la zona de seguridad).

Como se menciona anteriormente con referencia a las figuras 6 y 9, aunque en algunas realizaciones el eNB que aloja la célula de origen 78 puede tomar la decisión en si el eNB que aloja la célula de destino 79 o la célula de destino 79 está en la misma zona de seguridad que el eNB que aloja la célula de origen 78 o la célula de origen 78 en sí (y por ello si el K_{Enb} puede utilizarse después del traspaso del UE 42), en otras realizaciones la decisión se puede tomar por otro nodo en la red de comunicación (por ejemplo, otro nodo en el RAN, o un nodo en la red central). En estas realizaciones, en el paso 82 el eNB que aloja la célula de origen 78 puede indicar a ese nodo que el UE 42 puede traspasarse a una célula de destino 79, el nodo puede determinar si la célula de origen 78 y la célula de destino 79 están en la misma zona de seguridad (por ejemplo, examinando una lista de células/eNB que están en la misma zona de seguridad que la célula de origen 78), y proporcionar una indicación apropiada al eNB que aloja la célula de origen 78.

Además de determinar si la célula de destino 79 está en la misma zona de seguridad que la célula de origen 78, el eNB que aloja la célula de origen 78 puede además considerar si el UE soporta la característica (es decir, la habilidad de utilizar el K_{eNB} desde la célula de origen 78 en la célula de destino 79), y/o si el eNB que aloja la célula de destino 79 puede determinar si el UE 42 soporta la característica examinando las capacidades de UE que recibe como parte de la operación normal de LTE. El eNB que aloja la célula de origen 78 puede determinar si el eNB que aloja la célula de origen 79 soporta la característica durante el establecimiento de conexión X2 o utilizando datos de configuración RAN o durante el procedimiento de traspaso, por ejemplo.

Si en el paso 82 el eNB que aloja la célula de origen 78 determina que el K_{eNB} activo actualmente no puede utilizarse de forma segura en la célula de destino 79 (es decir, utilizando el K_{eNB} actual en la célula de destino 79 después del traspaso comprometerá la seguridad), el traspaso ocurrirá según técnicas convencionales (por ejemplo, como se describe anteriormente con referencia a la figura 1). Eso es, una nueva clave base, denotada K_{eNB}, se deriva por el eNB que aloja la célula de origen 78 para utilizar por el eNB que aloja la célula de destino 79 después del traspaso, y esta nueva clave base se manda al eNB que aloja la célula de destino 79.

De otra manera, si se determina en el paso 82 que el K_{eNB} activo actualmente puede utilizarse por el eNB que aloja la célula de destino 79 sin comprometer la seguridad, el eNB que aloja la célula de origen 78 informa que el eNB que aloja la célula de destino 79 sobre la decisión al mismo tiempo que proporciona el eNB que aloja la célula de destino 79 con el K_{eNB} en el mensaje petición de preparación de traspaso 84. Este mensaje 84 puede también incluir las capacidades de seguridad de UE, el valor de los conteos de protocolo de convergencia de datos de paquete (PDCP), y las identidades de los identificadores de portador de radio que se han utilizado para construir vectores de inicialización para el algoritmo de encriptación con el K_{eNB}.

Cuando el eNB que aloja la célula de destino 79 recibe esta información, el eNB que aloja la célula de destino 79 no realiza ninguna derivación adicional en el K_{eNB} recibido (que el eNB que aloja la célula de destino 79 de otra manera habría hecho según el procedimiento de traspaso convencional). Estas derivaciones de clave adicionales en el procedimiento de traspaso LTE convencional se refieren a la derivación realizada por el eNB que aloja la célula de destino 79 en un traspaso S1. En un traspaso S1, el eNB que aloja la célula de destino 79 recibe material de clave desde el MME y entonces realiza una derivación de ese material de clave junto con el PCI y EARFCN-DL de la célula maestra de destino para llegar a la clave base para utilizar en la célula de destino.

Después de tomar la decisión de si mantener el K_{eNB} después de que se haya hecho el traspaso, el eNB que aloja la célula de origen 78 directa o indirectamente informa al UE 42 de la decisión, es decir, si el K_{eNB} actualmente activo también debería utilizarse con la célula de destino 79. El eNB que aloja la célula de origen 78 puede informar al UE 42 de esto de un número de maneras diferentes.

En un primer ejemplo, donde el K_{eNB} actualmente activo debería mantenerse después del traspaso, el eNB que aloja la célula de destino 79 puede crear una orden de traspaso en la que el eNB que aloja la célula de destino 79 expresa que el K_{eNB} actualmente activo debería utilizarse también después del traspaso (es decir, no debe ocurrir ninguna derivación de clave horizontal o vertical) y que el mismo algoritmo de encriptación debe continuar para utilizarse. El objetivo de utilizar el mismo algoritmo de encriptación es asegurar que también la clave de encriptación derivada desde la clave base (K_{eNB}) se mantiene la misma antes y después del traspaso. Esto puede desearse en accesos como LTE donde la clave de encriptación está obligada al algoritmo de encriptación con el que se debe utilizar mediante una derivación de clave. Cualquier otro parámetro utilizado en la clave de encriptación puede también mantenerse igual para asegurar que la clave de encriptación no cambia en el traspaso. El eNB que aloja la célula de destino 79 puede enviar la orden de traspaso al eNB que aloja la célula de origen 78 para más transmisión al UE 42 en el mensaje de reconfiguración RRC 88.

En el segundo ejemplo, el eNB que aloja la célula de origen 78 puede incluir una indicación de la decisión de que puede pasar al UE 42 junto con la orden de traspaso en el mensaje de reconfiguración RRC 88.

En un tercer ejemplo, en vez de señalizar explícitamente el resultado de la decisión, el eNB que aloja la célula de origen 78 puede señalizar implícitamente el resultado de la decisión y si los mismos algoritmos de encriptación e integridad deberían utilizarse mediante otras combinaciones de elementos de información en los mensajes de traspaso. Por ejemplo, si no se pasa NCC y el UE 42 recibe un valor para un parámetro que está actualmente inutilizado según los estándares, el UE 42 puede deducir que la clave base activa actualmente (K_{eNB}), y el algoritmo de protección de integridad y encriptación también debería utilizarse en la célula de destino 79. Un posible ejemplo de dicho valor de parámetro inutilizado podría ser un número de algoritmo de encriptación 7 (que está actualmente indefinido en 3GPP TS 36.331 clausula 6.3.3. Si se pasa en NCC, no es posible reutilizar el K_{eNB}, ya que el paso del NCC indica que el eNB que aloja la célula de origen 78 ha derivado un K_{eNB} desde una clave NH fresca en una derivación vertical.

Cuando el UE 42 recibe el mansaje de reconfiguración RRC 88 (que incluye la orden de traspaso) determina, en base a la información en el mensaje al respecto de la decisión para reutilizar la clave base (K_{eNB}) que utiliza con el eNB que aloja la célula de origen 78, de si realizar una derivación de clave horizontal o vertical de la clave base (K_{eNB}) para determinar una nueva clave base, K_{eNB}, de si reutilizar el K_{eNB} activo actualmente para proteger las comunicaciones con el eNB que aloja la célula de destino 79. Por si acaso se debe realizar una derivación de clave vertical y horizontal, el UE 42 derivará la clave base (K_{eNB}) de la manera convencional como se prescribe en LTE. Sin embargo, si la clave base (K_{eNB}) se debe reutilizar, el UE 42 debería continuar utilizando la clave base actualmente activa (K_{eNB}) también en la célula de destino 79.

En algunas realizaciones, la instancia PDCP puede ser una función que es central tanto al eNB que aloja la célula de origen 78 como al eNB que aloja la célula de destino 79, en cuyo caso la clave base (K_{eNB}), PDCP cuenta y los identificadores portadores de radio utilizados no necesitan enviarse al eNB que aloja la célula de destino 79 por el eNB que aloja la célula de origen 78, y solo es necesario que el eNB que aloja la célula de origen 78 envíe al eNB que aloja la célula de destino 79 la información de que la clave base (K_{eNB}) y el algoritmo de encriptación se seguirán utilizando.

La figura 11 es un diagrama de bloques de un primer nodo de acceso de radio 40 según una realización. El primer nodo de acceso de radio 40 es para utilizar en una red de comunicación 32 y comprende un procesador 1101 y una memoria 1102. La memoria 1102 contiene instrucciones ejecutables por el procesador 1101 de manera que el primer nodo de acceso de radio 40 está operativo para determinar si una primera clave base que se utiliza para determinar una primera clave de encriptación para encriptar comunicaciones entre un dispositivo de comunicación 42 y el primer nodo de acceso de radio 40 puede utilizarse por el segundo nodo de acceso de radio 40 para determinar una segunda clave de encriptación para encripta comunicaciones entre el dispositivo de comunicación 42 y el segundo nodo de acceso de radio 40, y enviar la primera clave base al segundo nodo de acceso de radio 40 durante el traspaso del dispositivo de comunicación 42 desde el primer nodo de acceso de radio 40 al segundo nodo de acceso de radio 40 si la primera clave base puede utilizarse por el segundo nodo de acceso de radio 40.

La figura 12 es un diagrama de bloques de un dispositivo de comunicación 42 según otra realización. El dispositivo de comunicación 42 comprende un procesador 1201 y una memoria 1202. La memoria 1202 contiene instrucciones ejecutables por el procesador 1202, donde el dispositivo de comunicación 42 está operativo para recibir una indicación de si una primera clave base que se utilizó para determinar una primera clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación 42 y un primer nodo de acceso de radio 40 en una red de comunicación 32 puede utilizarse para determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación 42 y un segundo nodo de acceso de radio 40 en la red de comunicación 32 en el traspaso del dispositivo de comunicación 42 desde el primer nodo de acceso de radio 40 al segundo nodo de acceso de radio 40, determina una segunda clave de encriptación desde la primera clave base si la indicación recibida indica que la primera clave base puede utilizarse para determinar una segunda clave de encriptación; determina una segunda clave base desde la primera clave base si la indicación recibida no indica que la primera clave base puede utilizarse para determinar una segunda clave de encriptación, y determina una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación 42 y el segundo nodo de acceso de radio 40 desde la segunda clave base.

La figura 13 es un diagrama de bloques de un segundo nodo de acceso de radio 40 según una realización. El segundo nodo de acceso de radio 40 es para utilizar en una red de comunicación 32 y comprende un procesador 1201 y una memoria 1302. La memoria contiene instrucciones ejecutables por el procesador 1301 de manera que el segundo nodo de acceso de radio 40 está operativo para recibir una primera clave base desde un primer nodo de acceso de radio 40 en la red de comunicación 32 durante un traspaso de un dispositivo de comunicación 42 desde el primer nodo de acceso de radio 40 al segundo nodo de acceso de radio 40, recibir desde el primer nodo de acceso de radio 40 una indicación de un algoritmo de generación de clave de encriptación para utilizar para determinar una primera clave de encriptación desde la primera clave base; y determinar la primera clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación 42 y el segundo nodo de acceso de radio 42 desde la primera clave base utilizando el algoritmo de generación de clave de encriptación indicado.

La figura 14 es un diagrama de bloques de un nodo 36, 38 según una realización más. El nodo 36, 38 es para utilizar en una red de comunicación 32, y el nodo 36, 38 comprende un procesador 1401 y una memoria 1402. La memoria 1402 contiene instrucciones ejecutables por el procesador 1401 de manera que el nodo 36, 38 está operativo para recibir una petición desde un primer nodo de acceso de radio 40 en la red de comunicación 32 para información en un segundo nodo de acceso de radio 40 en la red de comunicación 42, la información que se refiere a si la primera clave base que se utilizó para determinar una primera clave de encriptación para encriptar comunicaciones entre un dispositivo de comunicación 42 y el primer nodo de acceso de radio 40 que puede utilizarse para determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación 42 y el segundo nodo de acceso de radio 40, y enviar información en el segundo nodo de acceso de radio 40 al primer nodo de acceso de radio 40, la información indicando si la primera clave base puede utilizarse por el segundo nodo de acceso de radio 40.

La figura 15 es un diagrama de bloques de un primer nodo de acceso de radio 40 según todavía a otra realización. El primer nodo de acceso de radio 40 se para utilizar en una red de comunicación 32 y comprende un primer módulo de determinación 1501 que se configura para determinar si una primera clave base que se utiliza para determinar una primera clave de encriptación para encriptar comunicaciones entre un dispositivo de comunicación 42 y el primer nodo de acceso de radio 40 se puede utilizar por un segundo nodo de acceso de radio 40 para determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación 42 y el segundo nodo de acceso de radio 40. El primer nodo de acceso de radio 40 también comprende un primer módulo de envío 1502 que está configurado para enviar una primera clave base a un segundo nodo de acceso de radio 40 durante un traspaso del dispositivo de comunicación 42 desde el primer nodo de acceso de radio 40 al segundo nodo de acceso de radio 40 si la primera clave base se puede utilizar por el segundo nodo de acceso de radio 40.

La figura 16 es un diagrama de bloques se un dispositivo de comunicación según todavía otra realización. El dispositivo de comunicación 42 comprende un módulo receptor 1601 que está configurado para recibir una indicación de si una primera clave base que se utilizó para determinar una primera clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación 42 y un primer nodo de acceso de radio 40 en una red de comunicación 32 se puede utilizar para determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación 42 y un segundo nodo de acceso de radio 40 en la red de comunicación 32 en el traspaso del dispositivo de comunicación 42 y un segundo nodo de acceso de radio 40 en la red de comunicación 32 en el traspaso del dispositivo de comunicación 42 desde el primer nodo de acceso de radio 40 al segundo nodo de acceso de radio 40, un primer módulo de determinación 1602 configurado para determinar una segunda clave de encriptación desde la primera clave base si la indicación recibida indica que la primera clave base puede utilizarse para determinar una segunda clave de encriptación; un segundo módulo de determinación 1603 configurado para determinar una segunda clave base desde la primera clave base si la indicación recibida no indica que la primera clave base puede utilizarse para determinar una segunda clave de encriptación; y un tercer módulo de determinación 1604 configurado para determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación 42 y el segundo nodo de acceso de radio 40 desde la segunda clave base.

La figura 17 es un diagrama de bloques de un segundo nodo de acceso de radio 40 según todavía otra realización. El segundo nodo de acceso de radio 40 es para utilizar una red de comunicación 32 y comprende un primer módulo receptor 1701 configurado para recibir una primera clave base desde un primer nodo de acceso de radio 40 en la red de comunicación 32 durante el traspaso de un dispositivo de comunicación 42 desde el primer nodo de acceso de radio 40 al segundo nodo de acceso de radio 40, un segundo módulo receptor 1702 configurado para recibir desde el primer nodo de acceso de radio 40 una indicación de un algoritmo de generación de clave de encriptación para utilizar para determinar una primera clave de encriptación desde la primera clave base; y un módulo de determinación 1703 configurado para determinar la primera clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación 42 y el segundo nodo de acceso de radio 40 desde la primera clave base utilizando el algoritmo de generación de clave de encriptación indicado.

La figura 18 es un diagrama de bloques de un nodo 36, 38 según todavía otra realización. El nodo 36, 38 es para utilizar en una red de comunicación 32, y comprende un módulo receptor 1801 configurado para recibir una petición desde un primer nodo de acceso de radio 40 en la red de comunicación 32 para información en un segundo nodo de acceso de radio 40 en la red de comunicación 32, la información que se refiere a si la primera clave base que se utilizó para determinar una primera clave de encriptación para encriptar comunicaciones entre un dispositivo de comunicación 42 y el primer nodo de acceso de radio 40 puede utilizarse para determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación 42 y el segundo nodo de acceso de radio 40, y un módulo de envío 1802 configurado para enviar información en el segundo nodo de acceso de radio 40 al primer nodo de acceso de radio 40, la información indicando si la primera clave base puede utilizarse por el segundo nodo de acceso de radio 40.

Como se menciona anteriormente, las técnicas descritas aquí pueden proporcionar un número de ventajas. Por ejemplo, las técnicas pueden: proporcionar más implementaciones eficientes de traspasos para eNB, proporcionar un traspaso más rápido y suave, proporcionar que una operadora configure la red para utilizar los recursos más eficientemente y no rebase la seguridad, soportar la virtualización/nubificación de las funciones de red con menos requisitos para la memoria intermedia y disminuir retrasos en el traspaso, y/o proporcionar la posibilidad de realizar traspasos no interrumpidos cuando se utiliza más de una portadora.

Modificaciones y otras variantes de las realizaciones descritas se le ocurrirán a alguien experto en la técnica que tiene el beneficio de las enseñanzas presentadas en las descripciones que vienen adelante y los dibujos asociados. Por ello, se debe entender que las realizaciones no deben limitarse a los ejemplos específicos divulgados y que se intenta que las modificaciones y otras variantes se incluyan dentro del alcance de esta divulgación. Aunque se empleen aquí diferentes términos, se utilizan en un sentido genérico y descriptivo y no con fines de limitación.

El alcance de la invención se define por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para operar un primer nodo de acceso de radio en una red de comunicación, comprendiendo el método:

determinar (601) si una primera clave base que se utiliza para determinar una primera clave de encriptación para encriptar comunicaciones entre un dispositivo de comunicación y el primer nodo de acceso de radio puede utilizarse por un segundo nodo de acceso de radio para determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y el segundo nodo de acceso de radio;

si la primera clave base puede utilizarse por el segundo nodo de acceso de radio, enviar (603) la primera clave base al segundo nodo de acceso de radio durante el traspaso del dispositivo de comunicación desde el primer nodo de acceso de radio al segundo nodo de acceso de radio; y

si la primera clave base no puede utilizarse por el segundo nodo de acceso de radio, determinar (605) una segunda clave base desde la primera clave base y enviar (607) la segunda clave base al segundo nodo de acceso de radio durante el traspaso del dispositivo de comunicación desde el primer nodo de acceso de radio al segundo nodo de acceso de radio.

2. Un método como se define en la reivindicación 1, en el que el método además comprende el paso de:

si la primera clave base puede utilizarse por el segundo nodo de acceso de radio, enviar una indicación al dispositivo de comunicación de que la primera clave base debe utilizarse para determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y el segundo nodo de acceso de radio.

3. Un método como se define en cualquiera de las reivindicaciones 1-2, en el que si se determina que la primera clave base no puede utilizarse por el segundo nodo de acceso de radio, el método además comprende el paso de:

enviar una indicación al dispositivo de comunicación para hacer que el dispositivo de comunicación determine una segunda clave base desde la primera clave base para utilizar con el segundo nodo de acceso de radio.

4. Un método como se define en cualquiera de las reivindicaciones 1-3, en el que el paso de determinar (601) si la primera clave base puede utilizarse por un segundo nodo de acceso de radio comprende determinar que la primera clave base puede utilizarse por el segundo nodo de acceso de radio si el primer nodo de acceso de radio y el segundo nodo de acceso de radio son parte de la misma zona de seguridad.

5. Un método como se define en la reivindicación 4, en el que el primer nodo de acceso de radio y el segundo nodo de acceso de radio son parte de la misma zona de seguridad si el primer nodo de acceso de radio y el segundo nodo de acceso de radio: (a) están funcionando como máquinas virtuales separadas en el mismo equipo físico informático; (b) son dos contenedores dentro de la misma máquina virtual; (c) están implementados en placas en el mismo estante físico; (d) se determina por política de seguridad que pertenecen a la misma zona de seguridad; o (e) están localizados físicamente en el mismo lugar.

6. Un método como se define en cualquiera de las reivindicaciones 1-5, en el que el paso de determinar (601) si la primera clave base puede utilizarse por un segundo nodo de acceso de radio comprende:

enviar una petición de información en el segundo nodo de acceso de radio a otro nodo en la red de comunicación; y

recibir información en el segundo nodo de acceso de radio desde dicho otro nodo, indicando la información si la primera clave base puede utilizarse por el segundo nodo de acceso de radio.

7. Un método como se define en cualquiera de las reivindicaciones 1-3, en el que el paso de determinar (601) si la primera clave base puede utilizarse por un segundo nodo de acceso de radio comprende:

examinar una lista o configuración local en el primer nodo de acceso de radio.

8. Un método como se define en cualquiera de las reivindicaciones 1-7, en el que el paso de enviar (603) la primera clave base al segundo nodo de acceso de radio durante el traspaso además comprende enviar una indicación de un algoritmo de generación de clave de encriptación que se utilizó para determinar la primera clave de encriptación desde la primera clave base.

9. Un método como se define en cualquiera de las reivindicaciones 1-8, en el que el primer nodo de acceso de radio y el segundo nodo de acceso de radio comparten un estado de protocolo de convergencia de datos de paquete, PDCP.

10. Un método de operar un dispositivo de comunicación, comprendiendo el método:

en traspaso del dispositivo de comunicación desde un primer nodo de acceso de radio en una red de comunicación a un segundo nodo de acceso de radio en la red de comunicación, recibir (701) una indicación de si una primera clave base que se utilizó para determinar una primera clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y el primer nodo de acceso de radio se puede utilizar para determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y el segundo nodo de acceso de radio;

si la indicación recibida indica que la primera clave base puede utilizarse para determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y el segundo nodo de acceso de radio, determinar (705) una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y el segundo nodo de acceso de radio desde la primera clave base;

de otra manera, determinar (707) una segunda clave base desde la primera clave base, y

determinar (709) una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y el segundo nodo de acceso de radio desde la segunda clave base.

11. Un método como se define en la reivindicación 10, en el que la indicación se recibe en un mensaje que se refiere al traspaso del dispositivo de comunicación desde el primer nodo de acceso de radio al segundo nodo de acceso de radio.

12. Un método como se define en la reivindicación 10 u 11, en el que la indicación se recibe desde el primer nodo de acceso de radio o el segundo nodo de acceso de radio.

13. Un primer nodo de acceso de radio (40) para utilizar en una red de comunicación (32), estando adaptado el primer nodo de acceso de radio para:

determinar si una primera clave base que se utiliza para determinar una primera clave de encriptación para encriptar comunicaciones entre un dispositivo de comunicación (42) y el primer nodo de acceso de radio puede utilizarse por un segundo nodo de acceso de radio (40) para determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y el segundo nodo de acceso de radio;

enviar la primera clave base al segundo nodo de acceso de radio durante el traspaso del dispositivo de comunicación desde el primer nodo de acceso de radio al segundo nodo de acceso de radio si la primera clave base puede utilizarse por el segundo nodo de acceso de radio; y

determinar una segunda clave base desde la primera clave base, si la primera clave base no puede utilizarse por el segundo nodo de acceso de radio (40), y enviar la segunda clave base al segundo nodo de acceso de radio durante el traspaso del dispositivo de comunicación (42) desde el primer nodo de acceso de radio al segundo nodo de acceso de radio.

14. Un primer nodo de acceso de radio (40) como se define en la reivindicación 13, en el que el primer nodo de acceso de radio está adaptado además para:

enviar una indicación al dispositivo de comunicación (42) de que la primera clave base se debe utilizar para determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y el segundo nodo de acceso de radio (40) si la primera clave base puede utilizarse por el segundo nodo de acceso de radio.

15. Un primer nodo de acceso de radio (40) como se define en cualquiera de las reivindicaciones 13-14, en el que el primer nodo de acceso de radio está adaptado además para:

enviar una indicación al dispositivo de comunicación (42) para hacer que el dispositivo de comunicación determine una segunda clave base desde la primera clave base para utilizar con el segundo nodo de acceso de radio (40) si determina que la primera clave base no puede utilizarse por el segundo nodo de acceso de radio.

16. Un primer nodo de acceso de radio (40) como se define en cualquiera de las reivindicaciones 13-15, en el que el primer nodo de acceso de radio está adaptado para determinar si la primera clave base puede utilizarse por un segundo nodo de acceso de radio (40) determinando que la primera clave base puede utilizarse por el segundo nodo de acceso de radio si el primer nodo de acceso de radio y el segundo nodo de acceso de radio son parte de la misma zona de seguridad.

17. Un primer nodo de acceso de radio (40) como se define en la reivindicación 16, en el que el primer nodo de acceso de radio y el segundo nodo de acceso de radio (40) son parte de la misma zona de seguridad si el primer nodo de acceso de radio y el segundo nodo de acceso de radio: (a) están funcionando como máquinas virtuales

separadas en el mismo equipo físico informático; (b) son dos contenedores dentro de la misma máquina virtual; (c) están implementados en placas en el mismo estante físico; (d) se determina por política de seguridad que pertenecen a la misma zona de seguridad; o (e) están localizados físicamente en el mismo lugar.

18. Un primer nodo de acceso de radio (40) como se define en cualquiera de las reivindicaciones 13-15, en el que el primer nodo de acceso de radio está adaptado para determinar si la primera clave base puede utilizarse por un segundo nodo de acceso de radio (40) por:

enviar una petición por información en el segundo nodo de acceso de radio a otro nodo en la red de comunicación (32); y

recibir información en el segundo nodo de acceso de radio desde dicho otro nodo, indicando la información si la primera clave base puede utilizarse por el segundo nodo de acceso de radio.

19. Un primer nodo de acceso de radio (40) como se define en cualquiera de las reivindicaciones 13-15, en el que el primer nodo de acceso de radio está adaptado para determinar si la primera clave base puede utilizarse por un segundo nodo de acceso de radio (40) por:

examinar una lista o configuración local en el primer nodo de acceso de radio.

20. Un primer nodo de acceso de radio (40) como se define en cualquiera de las reivindicaciones 13-19, en el que el primer nodo de acceso de radio está adaptado además para enviar una indicación de un algoritmo de generación de clave de encriptación que se utilizó para determinar la primera clave de encriptación desde la primera clave base.

21. Un primer nodo de acceso de radio (40) como se define en cualquiera de las reivindicaciones 13-20, en el que el primer nodo de acceso de radio y el segundo nodo de acceso de radio (40) comparten un estado de protocolo de convergencia de paquete de datos, PDCP.

22. Un dispositivo de comunicación (42), estando adaptado el dispositivo de comunicación para:

recibir una indicación de si una primera clave base que se utilizó para determinar una primera clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y un primer nodo de acceso de radio (40) en una red de comunicación (32) puede utilizarse para determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y un segundo nodo de acceso de radio (40) en la red de comunicación en el traspaso del dispositivo de comunicación desde el primer nodo de acceso de radio al segundo nodo de acceso de radio;

determinar una segunda clave de encriptación desde la primera clave base si la indicación recibida indica que la primera clave base puede utilizarse para determinar una segunda clave de encriptación;

determinar una segunda clave de encriptación desde la primera clave de encriptación si la indicación recibida no indica que la primera clave base puede utilizarse para determinar una segunda clave de encriptación; y

determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y el segundo nodo de acceso de radio desde la segunda clave base.

23. Un dispositivo de comunicación (42) como se define en la reivindicación 22, en el que la indicación es recibida en un mensaje que se refiere al traspaso del dispositivo de comunicación desde el primer nodo de acceso de radio (40) al segundo nodo de acceso de radio (40).

24. Un dispositivo de comunicación (42) como se define en la reivindicación 22 o 23, en el que la indicación se recibe desde el primer nodo de acceso de radio (40) o el segundo nodo de acceso de radio (40).

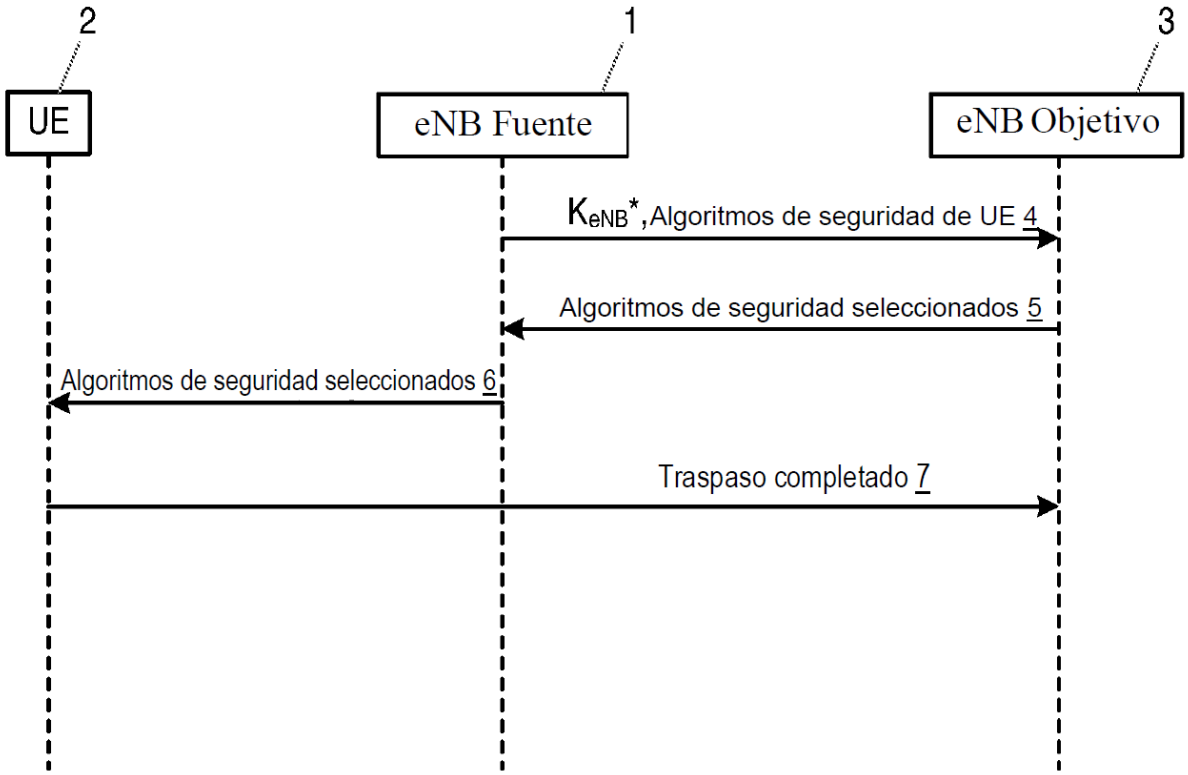
2
1
3
UE
eNB Fuente
eNB Objetivo
K_{eNB}^*,Algoritmos de seguridad de UE 4
Algoritmos de seguridad seleccionados 5
Algoritmos de seguridad seleccionados 6
Traspaso completado 7

Figura 1

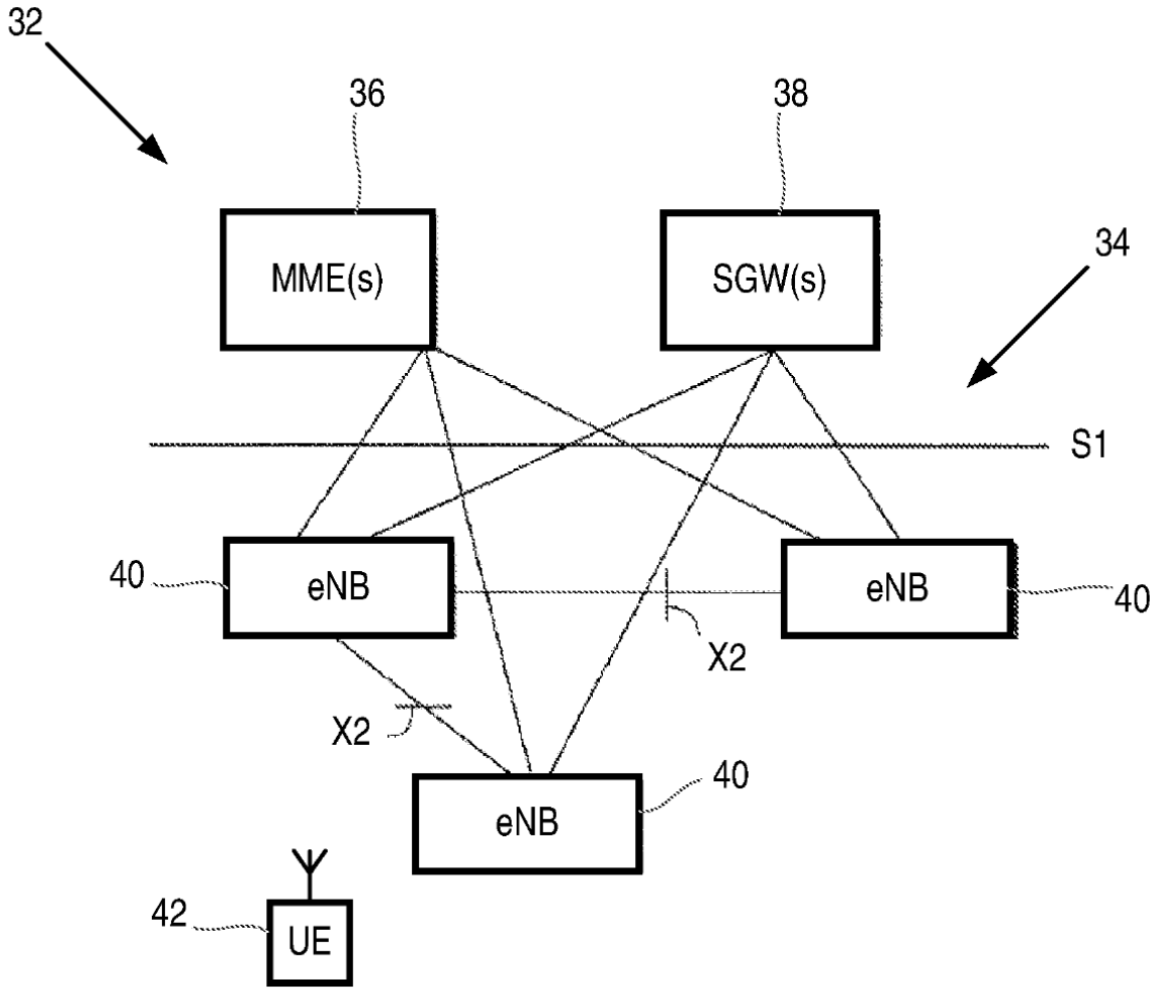

Figura 2

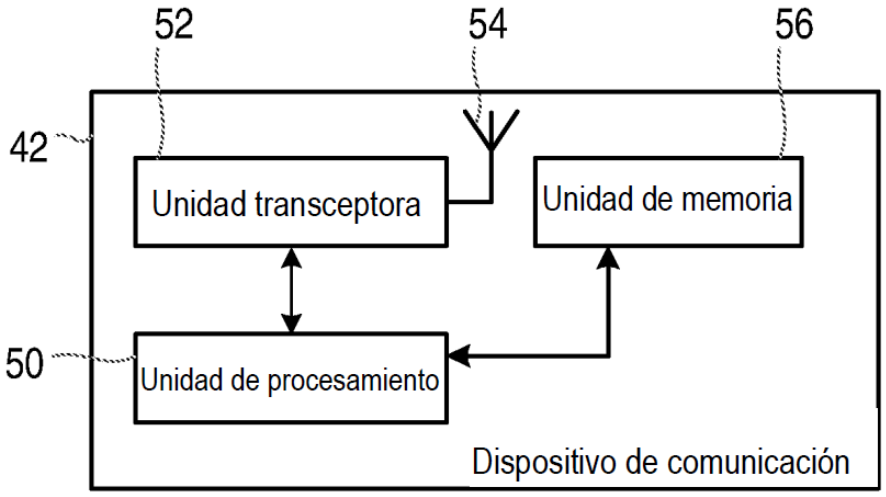

Figura 3

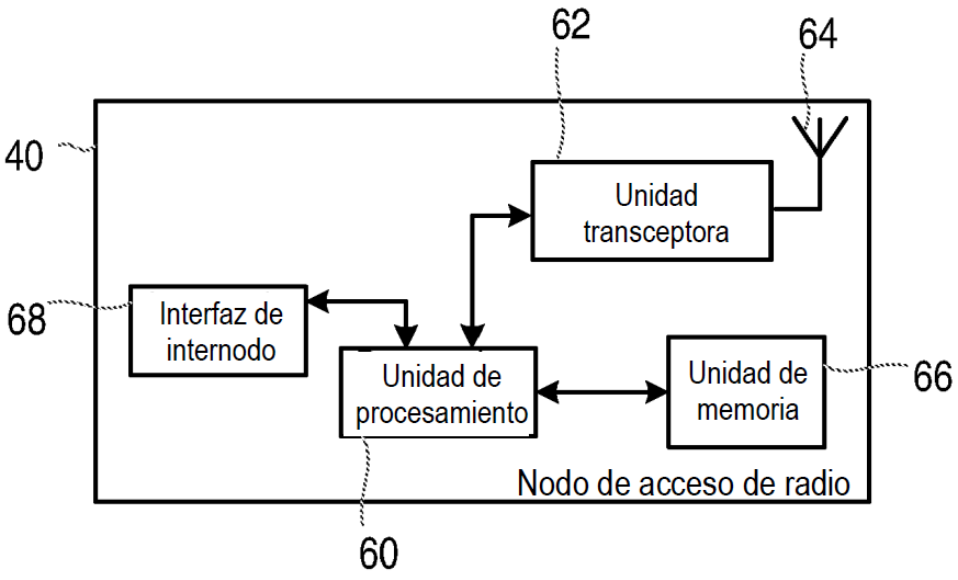

Figura 4

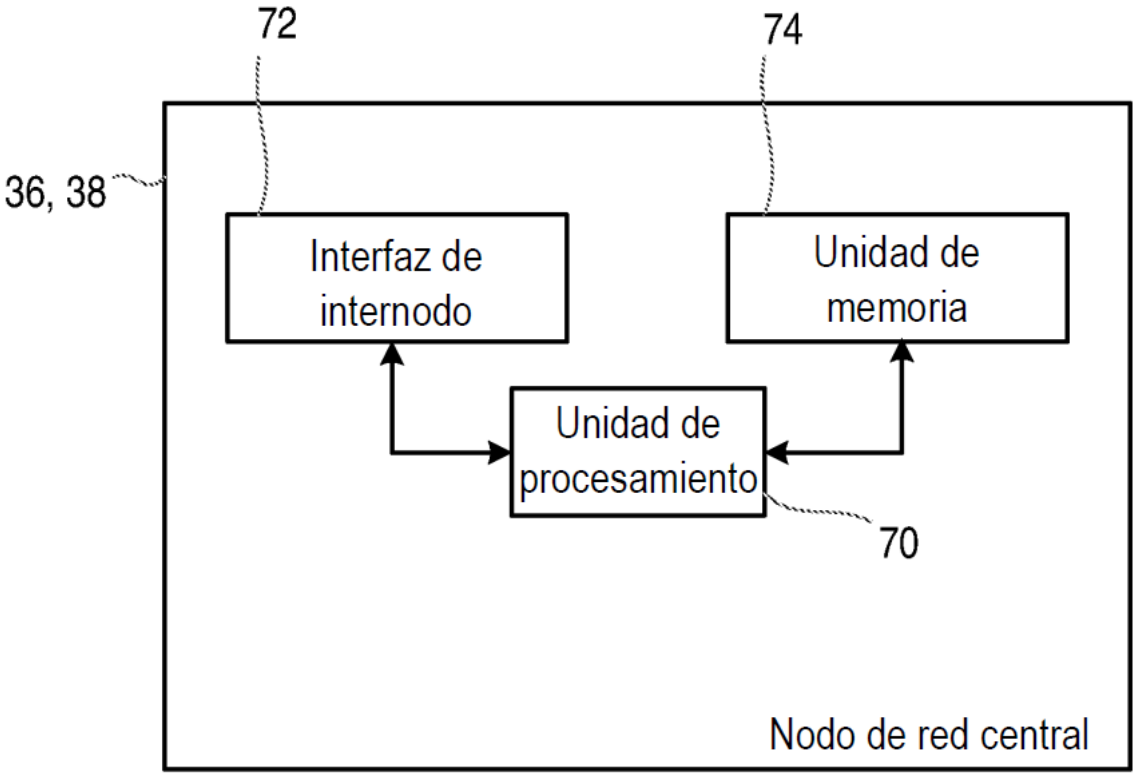
72
74
36, 38
Interfaz de internodo
Unidad de memoria
Unidad de procesamiento
70
Nodo de red central

Figura 5

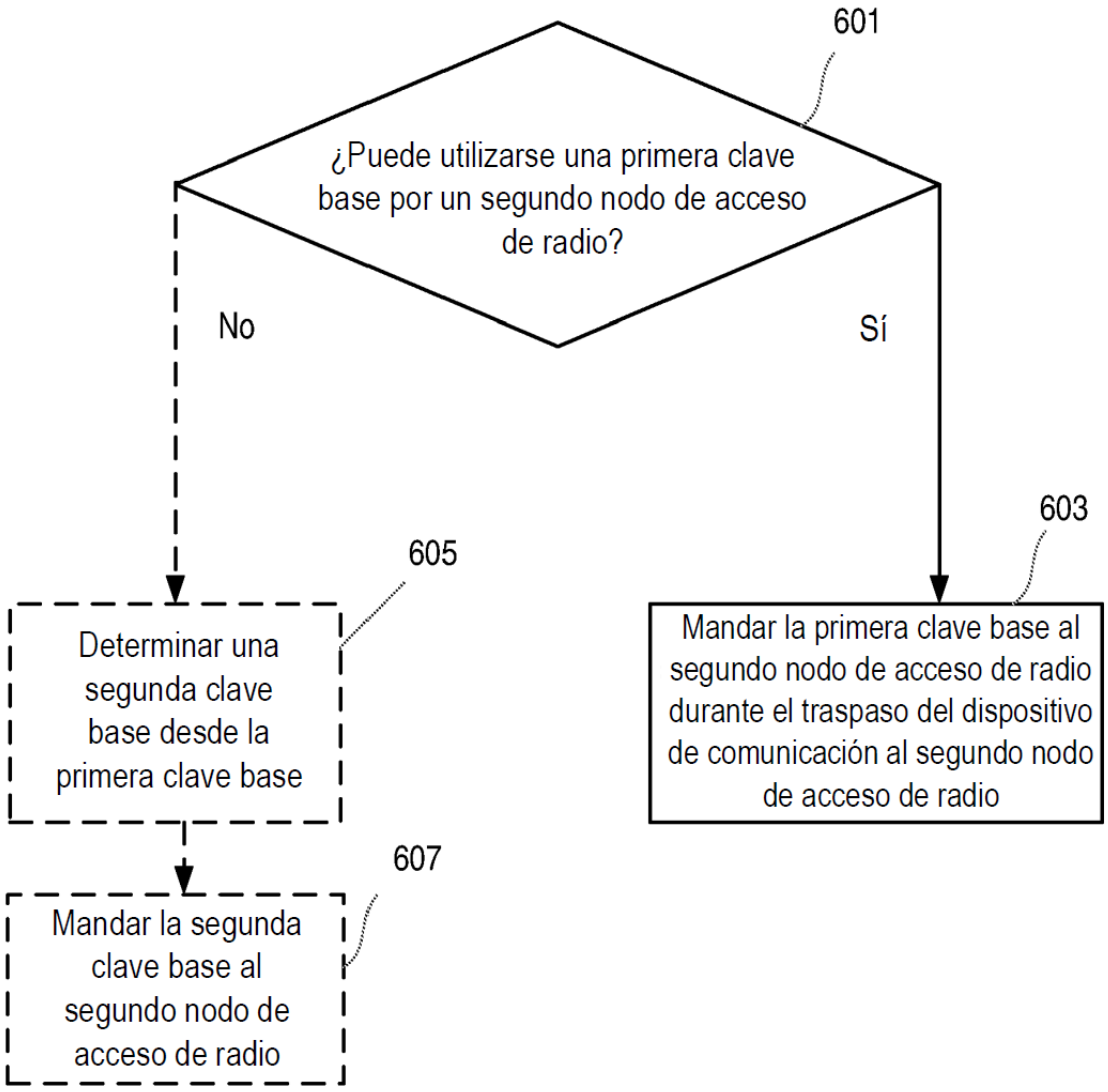
601
¿Puede utilizarse una primera clave base por un segundo nodo de acceso de radio?
No
Sí
603
Mandar la primera clave base al segundo nodo de acceso de radio durante el traspaso del dispositivo de comunicación al segundo nodo de acceso de radio
605
Determinar una segunda clave base desde la primera clave base
607
Mandar la segunda clave base al segundo nodo de acceso de radio

Figura 6

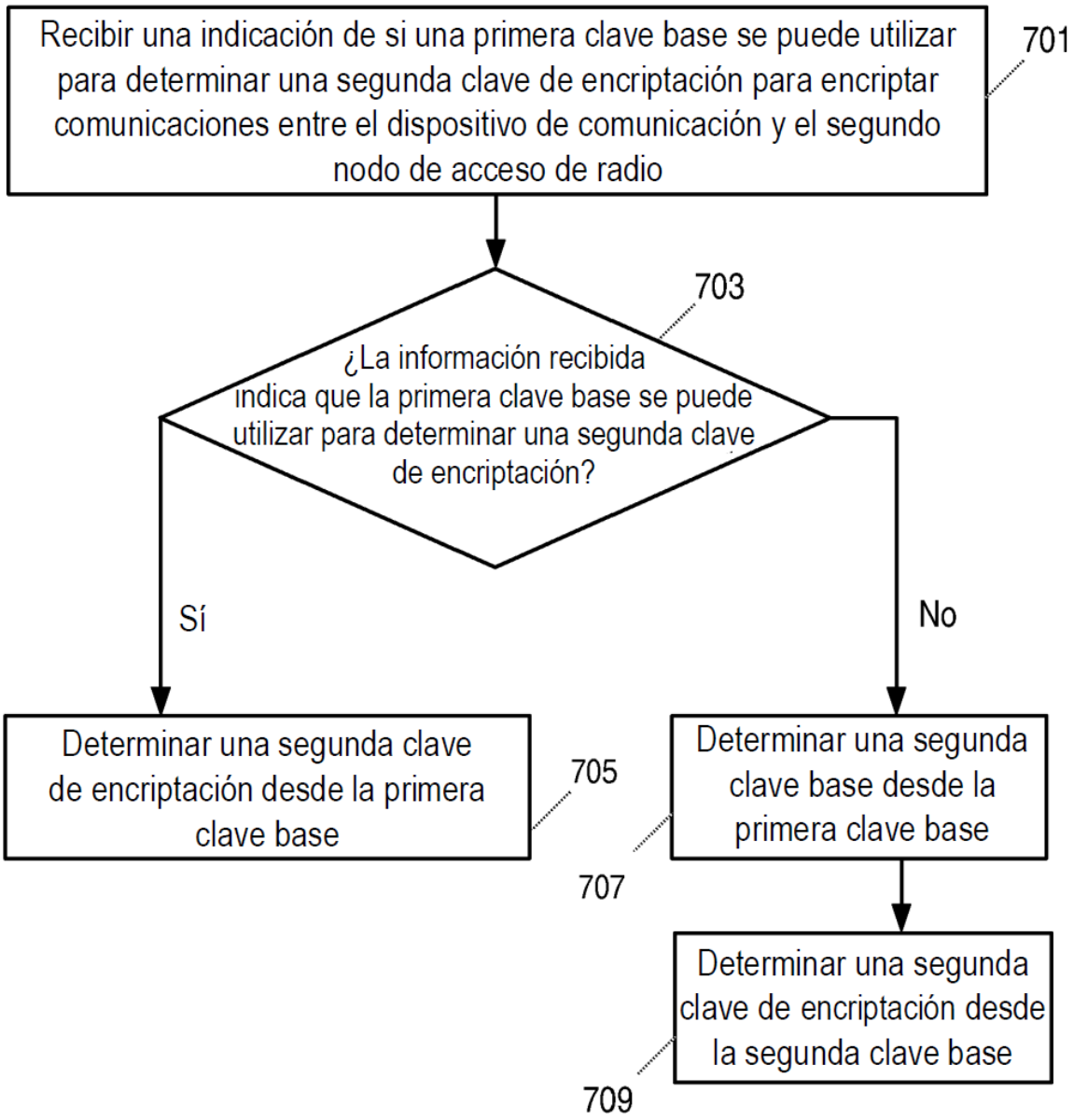
Recibir una indicación de si una primera clave base se puede utilizar para determinar una segunda clave de encriptación para encriptar comunicaciones entre el dispositivo de comunicación y el segundo nodo de acceso de radio
701
703
¿La información recibida indica que la primera clave base se puede utilizar para determinar una segunda clave de encriptación?
Sí
No
Determinar una segunda clave de encriptación desde la primera clave base
705
Determinar una segunda clave base desde la primera clave base
707
Determinar una segunda clave de encriptación desde la segunda clave base
709

Figura 7

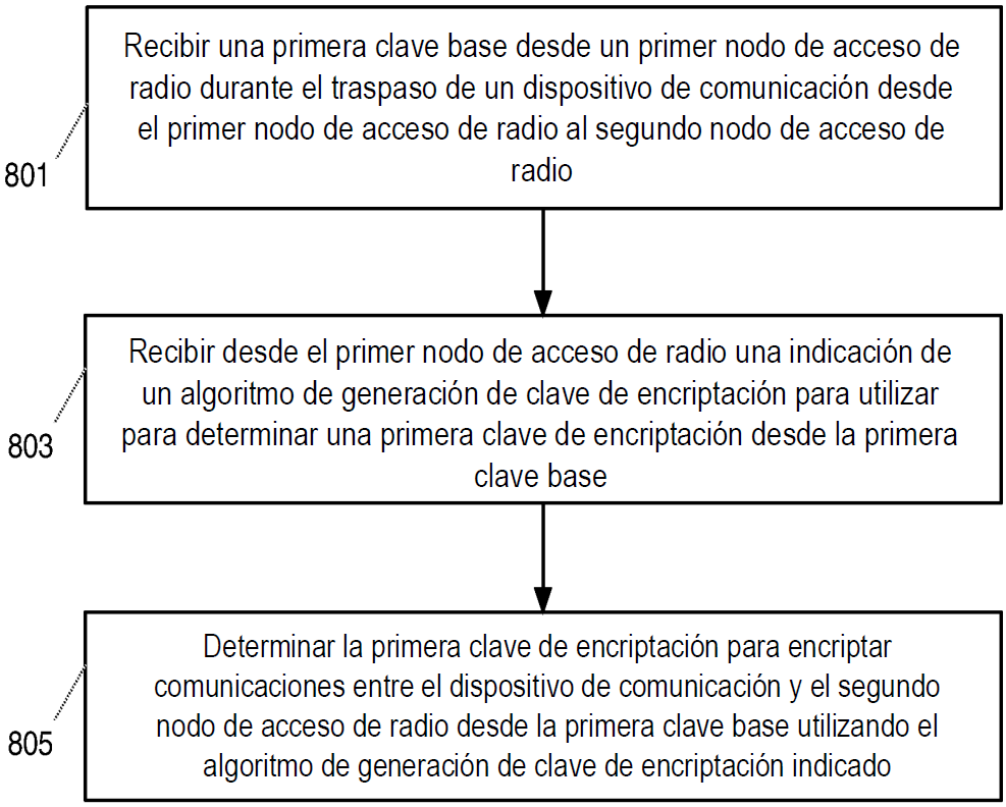

Figura 8

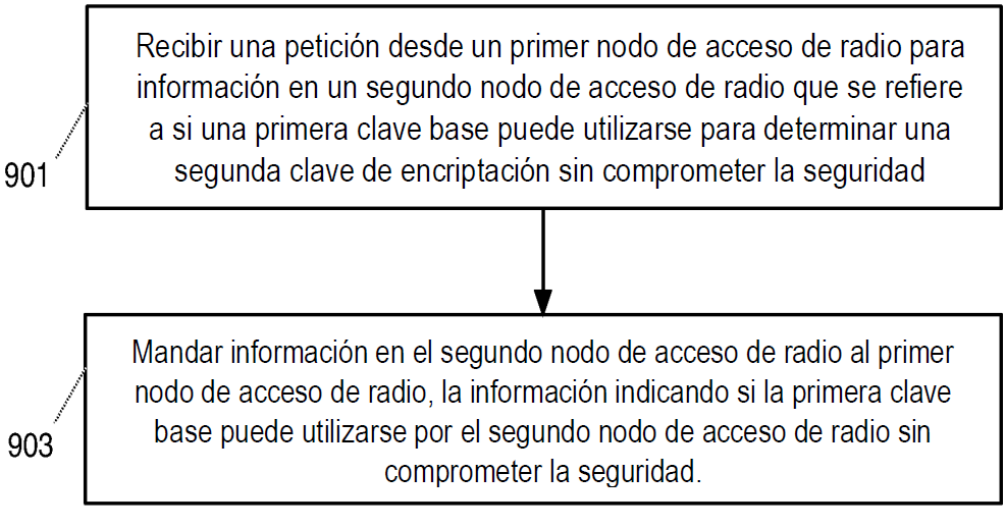

Figura 9

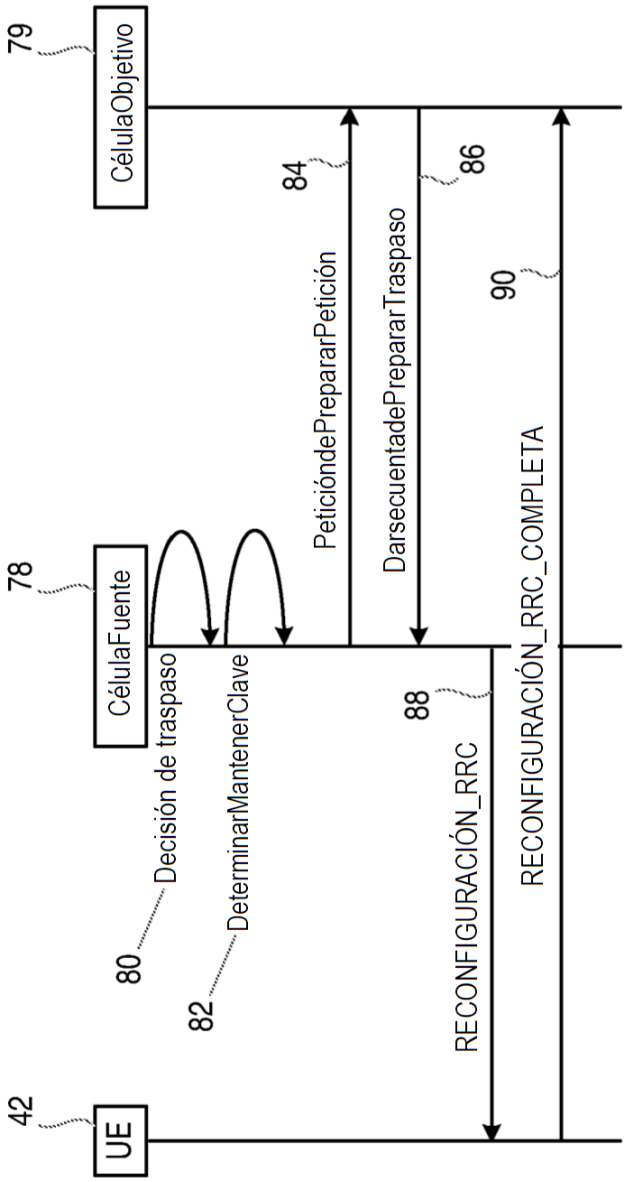
79
CélulaObjetivo
84
86
90
PeticióndePrepararPetición
DarsecuentadePrepararTraspaso
78
CélulaFuente
80
Decisión de traspaso
82
DeterminarMantenerClave
88
RECONFIGURACIÓN_RRC
RECONFIGURACIÓN_RRC_COMPLETA
42
UE

Figura 10

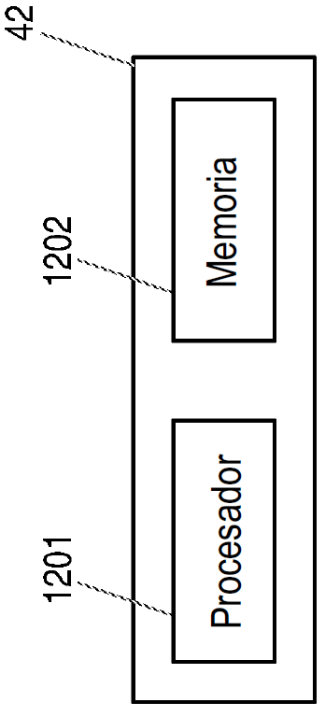

Figura 12

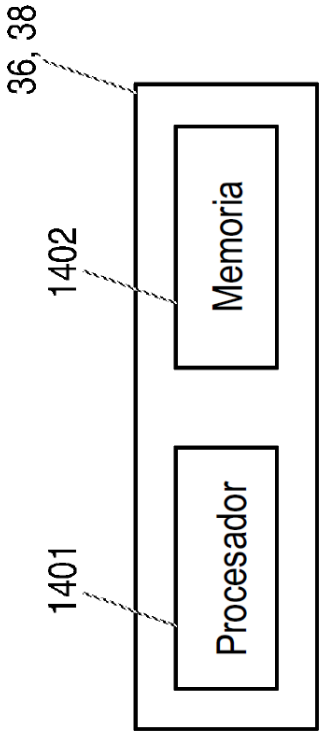

Figura 14

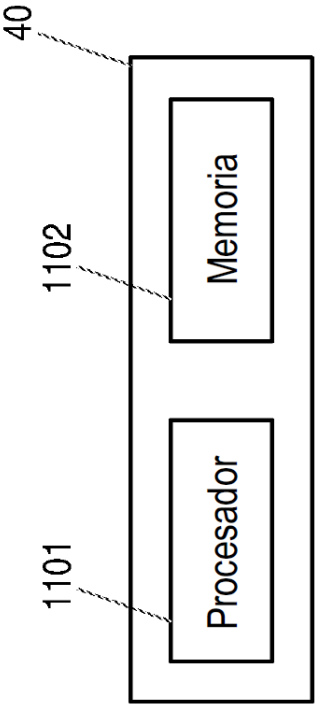

Figura 11

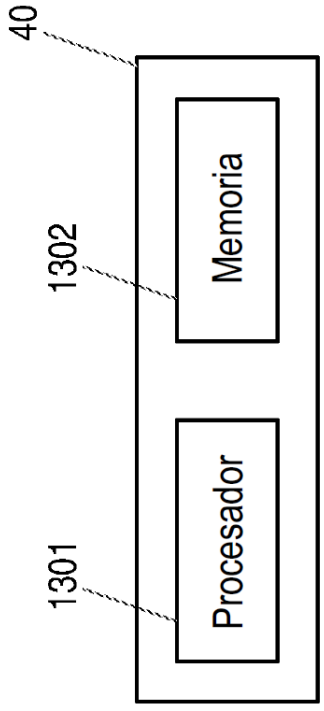

Figura 13

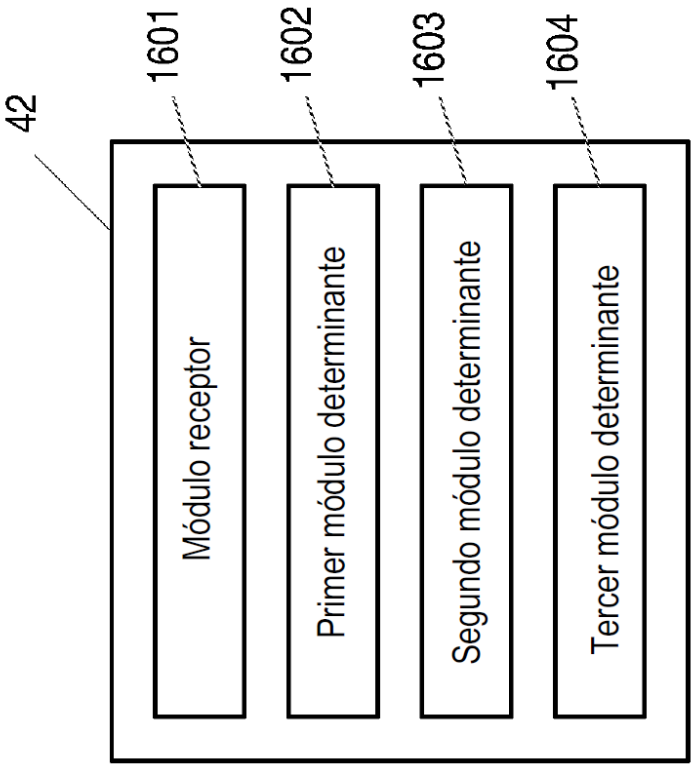

Figura 16

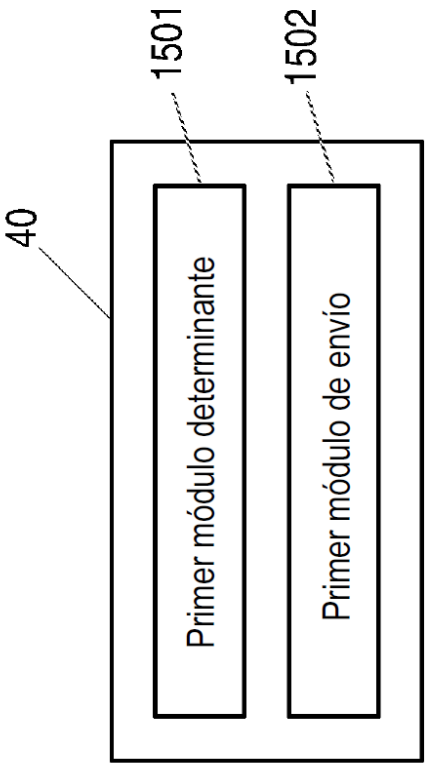

Figura 15

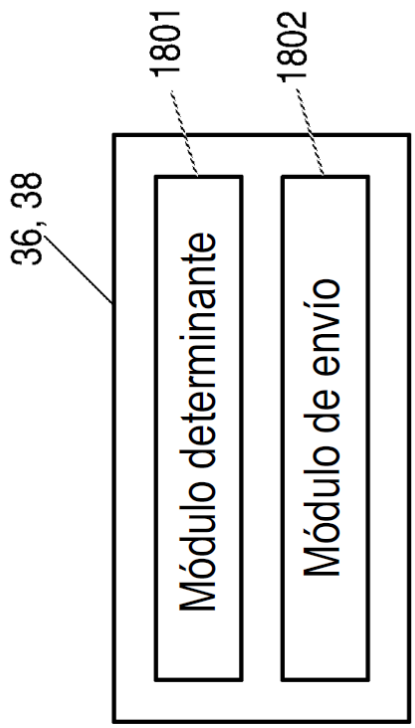

Figura 18

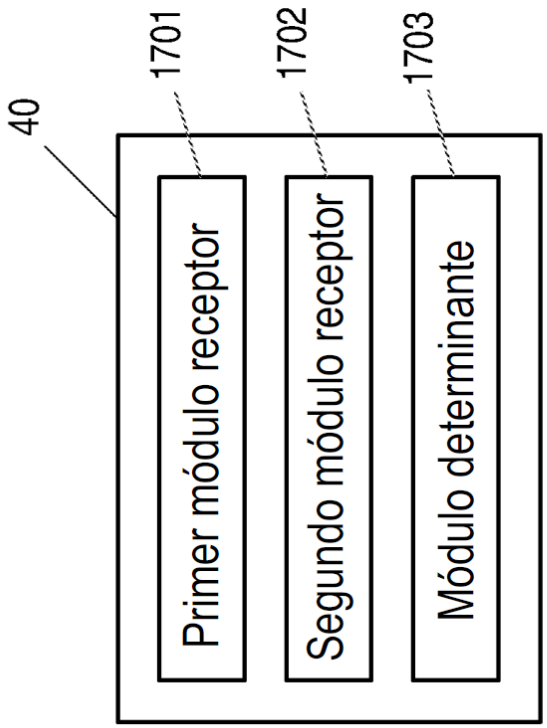

Figura 17